



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/445,132	03/13/2000	AHMET MURSIT ESKICIOGLU	RCA88637	9525

24498 7590 10/03/2005
THOMSON LICENSING INC.
PATENT OPERATIONS
PO BOX 5312
PRINCETON, NJ 08543-5312

EXAMINER

KIM, JUNG W

ART UNIT PAPER NUMBER

2132

DATE MAILED: 10/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/445,132

Applicant(s)

ESKICIOGLU ET AL.

Examiner

Jung W. Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 July 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5 and 7-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 10 is/are allowed.
- 6) ☒ Claim(s) 1-5, 7-9 and 11-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 7/05.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____.

AT

DETAILED ACTION

1. This Office action is in response to the amendment filed on July 27, 2005.
2. Claims 1-5 and 7-22 are pending.
3. Claims 1-5, 7, 8 and 10 are amended.
4. Claim 6 is canceled.
5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Information Disclosure Statement

6. The items listed on the information disclosure statement filed July 27, 2005 has been considered.

Response to Amendment

7. The 101 rejections to claims 1-10 are withdrawn as the amendment overcomes the 101 rejections.

Response to Arguments

8. Applicant's arguments with respect to the 112/1st paragraph rejections of claims 1-10 have been fully considered and are persuasive. The 112/1st paragraph rejections of claims 1-10 has been withdrawn.

Art Unit: 2132

9. Applicant's arguments with regards to the 103(a) rejections to claims 1-5 and 11-20 (Remarks, pgs. 12-15) have been fully considered but they are not persuasive.

10. In response to applicant's arguments that the Schneier reference (pg. 54) does not show all the features of the claimed invention (Remarks, pg. 12, 1st full paragraph), examiner disagrees. The first and second private keys associated with the second device are taught by Schneier as a combination of two teachings: authentication using public keys (the second device and an associated first private key) and the certification of public key using certificates (public key values are certified in certificates, which are signed using a private key of the certificate issuer; the private key of the certificate issuer is associated with the second device by virtue of the fact that the issuer is a subscriber of the certificate (assuming the certificate issuer and the certificate subscriber are not one and the same; if they are one and the same, then the rejection still holds).

11. Applicant later argues the following:

even assuming argenudo that the separate teachings within Schneier can be combined as suggested by the Examiner, modifying the example on page 54 of Schneier to use a digital certificate to certify a public key still fails to teach or suggest the claimed use of first and second private keys associated with the recited second device ... [m]odifying the example on page 54 of Schneier such that the host uses a certificate to acquire a certified public key, instead of merely looking one up in its database, does not teach the claim limitation of first and second private keys associated with the second party as recited in present Claim 1. The key used to sign the certificate is merely a private key associated with the certificate authority and not the certificate holder. (Remarks, pg. 13, 2nd full paragraph).

12. In response, first, as argued above, a certificate issuer private key used to sign the certificate that is issued to a certificate holder, does in fact fall under the scope of the private key being associated with the second party, since a certificate holder subscribes to the certificate authority: any signing key of the certificate authority to validate the certificate is "associated" with the certificate holder.

13. Second, the distinction of whether the secondary device fulfills the role of only a certificate subscriber separate from a certificate issuer, or whether the secondary device acts as both certificate subscriber and the certificate issuer does not make a patentable distinction, since the consolidation of multiple roles or features are obvious enhancements. In re Larson 144 USPQ 347 (CCPA 1965).

14. Hence, the prior art of record covers the limitations of claims 1-5 and 10-20.

Examiner Initiated Interview

15. In the Remarks of the amendment received on July 27, 2005, Applicant indicates that claims 21 and 22 incorporates the subject matter of cancelled claim 6 ("New Claim 22 incorporates the subject matter of now cancelled Claim 6, and the base and intervening claims from which Claim 6 depends. Accordingly, Applicants respectfully submit Claim 22, and claims 7-9, which depend from Claim 22, are in condition for allowance ... New Claim 21 incorporates the subject matter of now cancelled Claim 6 and Claim 1, the base claim upon which now cancelled Claim 6 ultimately depended." [pg. 8, 1st paragraph]). However, Claims 21 and 22 are broader than the subject matter of claims 1 and 6; particularly, claims 21 and 22 define the steps of encrypting the first

Art Unit: 2132

message using a public key to generate a second encrypted message; and sending data indicative of the second encrypted message to the second electronic device; claim 6 define the steps of encrypting the first message using the second public key related to the second private key of the second device to generate a second encrypted message; and sending data indicative of second encrypted message to the second electronic device. In a telephone interview with Paul P. Kiel, on September 15, this matter was discussed. It was determined that the broader scope was unintentional and that the original subject matter of claim 1 and now canceled claim 6 was being solicited. Examiner suggested changes to claims 21 and 22 to bridge the difference in scope.

Claim Rejections - 35 USC § 112

16. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

17. Claims 7-9, 21 and 22 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claims 21 and 22 recite the following steps:

- a. establishing a communication channel between a first and second electronic devices in response to the authentication of the second electronic device;

Art Unit: 2132

- b. encrypting the first message data using a public key to generate a second encrypted message data; and
- c. sending the second encrypted message data to the second electronic device.

However, the specification only enables establishing a communication channel between a first and second electronic devices in response to the authentication of the second electronic device after the first device sends confirmation of the authentication back to the second device, which include encrypting the first message data using a public key to generate a second encrypted message data and sending the second encrypted message data to the second electronic device (Specification, pg. 11, lines 15-24).

18. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

19. Claims 7-9, 21 and 22 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are: encrypting the first message data using the second public key related to the second devices second private key to generate a second encrypted message. This step defines a feature of confirming the authentication by the first device to the second device as enabled by the specification; an arbitrary public key to generate a second encrypted message does not enable a confirmation of the authorization, since only the second

public key stored in the encrypted certificate verifies that the decryption of encryption certificate by the first device was successful (Specification, pg. 11, lines 15-24).

Claim Rejections - 35 USC § 103

20. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, Applied Cryptography, Chapter 3, "Basic Protocols" and Chapter 24 "Example Implementations" (hereinafter Schneier).

21. As per claims 1, 3 and 4, Schneier discloses a method for managing access to a device (pgs. 53-54, "Authentication Using Public-Key Cryptography", especially, first four steps), the method comprising:

- d. sending a first message from a first electronic device to a second electronic device (pg. 54, step 1; implicit in the teaching of the two parties "the host" and "Alice" are network devices configured as a sender and receiver of a secured transmission; see also pg. 52, 1st paragraph under section 3.2 "Authentication", all subsequent authentication protocols are defined between computing devices);
- e. receiving from the second electronic device at the first electronic device the first message encrypted using a second private key of the second electronic device (pg. 54, steps 1 and 2);
- f. authenticating the second electronic device in response to the first encrypted message, wherein the step of authenticating comprises the steps of:

- i. decrypting the first encrypted message using the second public key to generate a first decrypted message; and comparing the first decrypted message to the first message (pg. 54, steps 3 and 4); and
- g. establishing a communication channel between the first and second electronic devices in response to the authentication of the second electronic device (pg. 54, step 4; Alice has access to the host's system in response to a successful authentication of Alice).

22. The authentication scheme does not disclose the use of digital certificates wherein the certificate comprises second identification data associated with the second device and a second public key of the second device, wherein the second device encrypts the digital certificate using a first private key of the second device, and wherein the step of authenticating includes the step of decrypting the digital certificate at the first device using a first public key then using the second public key of the second device to decrypt the first encrypted message. Schneier discloses the use of digital certificates wherein the certificate comprises identification data associated with a party and a public key of a party, wherein once a received digital certificate is authenticated, the public key stored in the digital certificate is validated and used for cryptographic processing. Schneier, pg. 574, last sentence; pg. 575-576 'Certificates', especially 3rd full paragraph; the authentication of the certificate requires a first private key to seal and sign the certificate and a first public key to authenticate the certificate. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to use a digital certificate to certify a public key, wherein prior to using the certified public key,

Art Unit: 2132

the digital certificate is authenticated using a public key to verify the signature on the digital certificate since it certifies a specific public key with a specific user. Schneier, pg. 575, 1st full paragraph. The aforementioned cover the limitations of claims 1, 3 and 4.

23. As per claim 2, the rejections of claims 1, 3 and 4 are incorporated herein. In addition, first identification is a necessary feature of a first message to establish a secure communication by means of an authenticated handshake. Although Schneier does not expressly teach including a data and a timestamp in the first message in the example disclosed, it is notoriously well-known in the art at the time the invention was made to incorporate a timestamp and date within a transmitted message. Examiner takes Official Notice of this teaching. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the first message to further comprise a time stamp and date since this feature prevents the message from being used in a replay attack as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 2.

24. As per claim 5, the rejections of claims 1, 3 and 4 are incorporated herein. In addition, since the first public key is available in the public domain, it would be obvious at the time the invention was made to store the first public key in the first device since it eliminates secure retrieval of the second device's public key for each secure connection between the first and second device as known to one of ordinary skill in the art. MPEP 2144.04.II. The aforementioned cover the limitations of claim 5.

25. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, and further in view of Ohashi et al. U.S. Patent No. 5,761,309 (hereinafter Ohashi).

26. As per claim 11, the rejections of claims 1-5 are incorporated herein. Schneier does not teach the method as managing access between a service provider and a set-top box having a smart card coupled thereto, wherein authentication occurs between the set-top box and a smart card and then a set-top box and a service provider. Arnold discloses a method for authenticating a cryptographic link between a service provider and a client terminal using a smart card coupled thereto by means of certificate authentication. (Ohashi, figures 2-4 and 7-10, and related text) It would be obvious to one of ordinary skill in the art at the time the invention was made to integrate the challenge routine covered by Schneier in a connected system between a service provider and a set-top box authenticated with a smart card since it enables services provided by the service provider to be restricted based on user rights and privileges stored on the smart card and actuated by a set-top box. Ohashi, *ibid*. The aforementioned cover the limitations of claim 11.

27. Claims 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Ohashi, and further in view of Force et al. U.S. Patent No. 5,533,123 (hereinafter Force).

28. As per claims 12-20, the rejections of claims 1-5 and 11 under 35 U.S.C. 103(a) are incorporated herein. Schneier does not expressly disclose the smart card comprising a plurality of digital certificates, each certificate containing service provider identification. Force discloses a smart card designed to incorporate multiple types of information, including a plurality of certificates, each certificate identifying a distinct service. (Force, col. 3:22-31) It would be obvious to one of ordinary skill in the art at the time the invention was made for the smart card to carry a plurality of certificates, wherein each certificate contains service provider information since it enables access to a plurality of services using only one smart card. Force, *ibid*. Moreover, in the ISO Authentication framework, independent certificate authorities issue digital certificates (Schneier, pg. 575, 1st full paragraph; Figure 24.3); and digital signatures in the ISO framework are tamper-resistant by means of an issuer signature on a hash of the certificate (digital certificates are secure in the public domain); hence, storage of a digital certificate at the service provider is an obvious enhancement since it eliminates the retrieval of the certificate by the provider for each authentication handshake with a set-top box. MPEP 2144.04.II. The aforementioned cover the limitations of claims 12-20.

Allowable Subject Matter

29. Claim 10 is allowed.

Art Unit: 2132

30. The subject matter defined in claims 7-9, 21 and 22 are not covered by the teachings of the prior art of record.

Conclusion

31. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

32. The Japanese foreign patent publication document no. 9-7708 discloses a method of authenticating two terminals to establishing a communication channel by means of the following steps:

- h. Terminals A and B receiving certificates Ca and Cb from a certificate authority, certifying respective public keys PUa and PUB; PRa and PRb are the respective private keys for A and B.
- i. Terminals A and B exchanging certificates and verifying the exchanged certificates (both certificates are signed by the certificate authority using its private key).
- j. Terminal A creating a random number Ra and encrypting Ra with PUB and signs the resulting encrypted value with PRa.
- k. Terminal A transmitting the encrypted value and signature data to terminal B.
- l. Terminal B decrypting the encrypted Ra with PRb and verifies the signature data using PUa.

Art Unit: 2132

- m. Terminal B then creating a random number R_b , creating a secret shared key by XOR operation on R_b and R_a ; encrypting R_b using P_{Ua} and signs the encrypted R_b using PR_b .
- n. Terminal B transmitting the encrypted value and signature data to terminal A.
- o. Terminal A decrypting the encrypted R_b using PR_a and verifying the signature data using P_{Ub} ; then creating the secret shared key by XOR operation on R_b and R_a , thereby providing the shared secret key securely between A and B.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

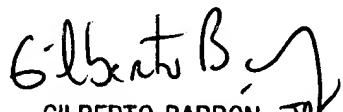
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



September 26, 2005

Jung W Kim
Examiner
Art Unit 2132



GILBERTO BARRON JK
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100